WHAT IS CLAIMED IS:

1. An encryption circuit, comprising:

a plurality of operation circuits which are connected; and

a control circuit controlling said plurality of operation circuits to provide encryption or decryption control; wherein

each of said plurality of operation circuits includes

a first register holding operation data,

an addition and subtraction circuit performing addition and subtraction with respect to the operation data held in said first register,

a right-shift circuit performing right-shift with respect to an operation result by said addition and subtraction circuit, and

a second register holding an operation result by said right-shift circuit;

an addition and subtraction circuit in a first operation circuit performs addition and subtraction using a carry-in signal from a second operation circuit, and outputs a carry-out signal generated through addition and subtraction to a third operation circuit; and

a right-shift circuit in said first operation circuit performs right-shift using a shift-in signal from said third operation circuit, and outputs a shift-out signal generated through right-shift to said second operation circuit.

2. The encryption circuit according to claim 1, wherein

said control circuit divides the operation data, and stores the data in the first register in said plurality of operation circuits.

3. The encryption circuit according to claim 1, wherein

said addition and subtraction circuit in said first operation circuit determines the operation data at a first clock, and

an addition and subtraction circuit in said third operation circuit determines the operation data and a carry-out from said first operation circuit at a second clock delayed by one clock from said first clock.

4. The encryption circuit according to claim 1, wherein

said addition and subtraction circuit in said first operation circuit determines the operation data at the first clock, and

in the second register in said first operation circuit, a bit except for a most significant bit is written at the second clock delayed by one clock from said first clock, and the most significant bit is written at a third clock delayed by half clock from said second clock.

5. The encryption circuit according to claim 1, wherein

said plurality of operation circuits are connected such that a carry-out signal and a shift-out signal form a loop.

6. The encryption circuit according to claim 1, wherein

respective one of said plurality of operation circuits further includes a left-shift circuit performing left-shift with respect to the operation result held in said second register, and

a left-shift circuit in said first operation circuit performs left-shift using a shift-in signal from said second operation circuit, and outputs a shift-out signal generated through left-shift to said third operation circuit.

7. The encryption circuit according to claim 6, wherein

said first operation circuit further includes a selector selectively outputting a shift-in signal from said third operation circuit and a shift-in signal from the left-shift circuit in said first operation circuit to the addition and subtraction circuit in said first operation circuit.